aviatrix

ACE

Aviatrix Certified Engineer

ThreatIQ and CostIQ

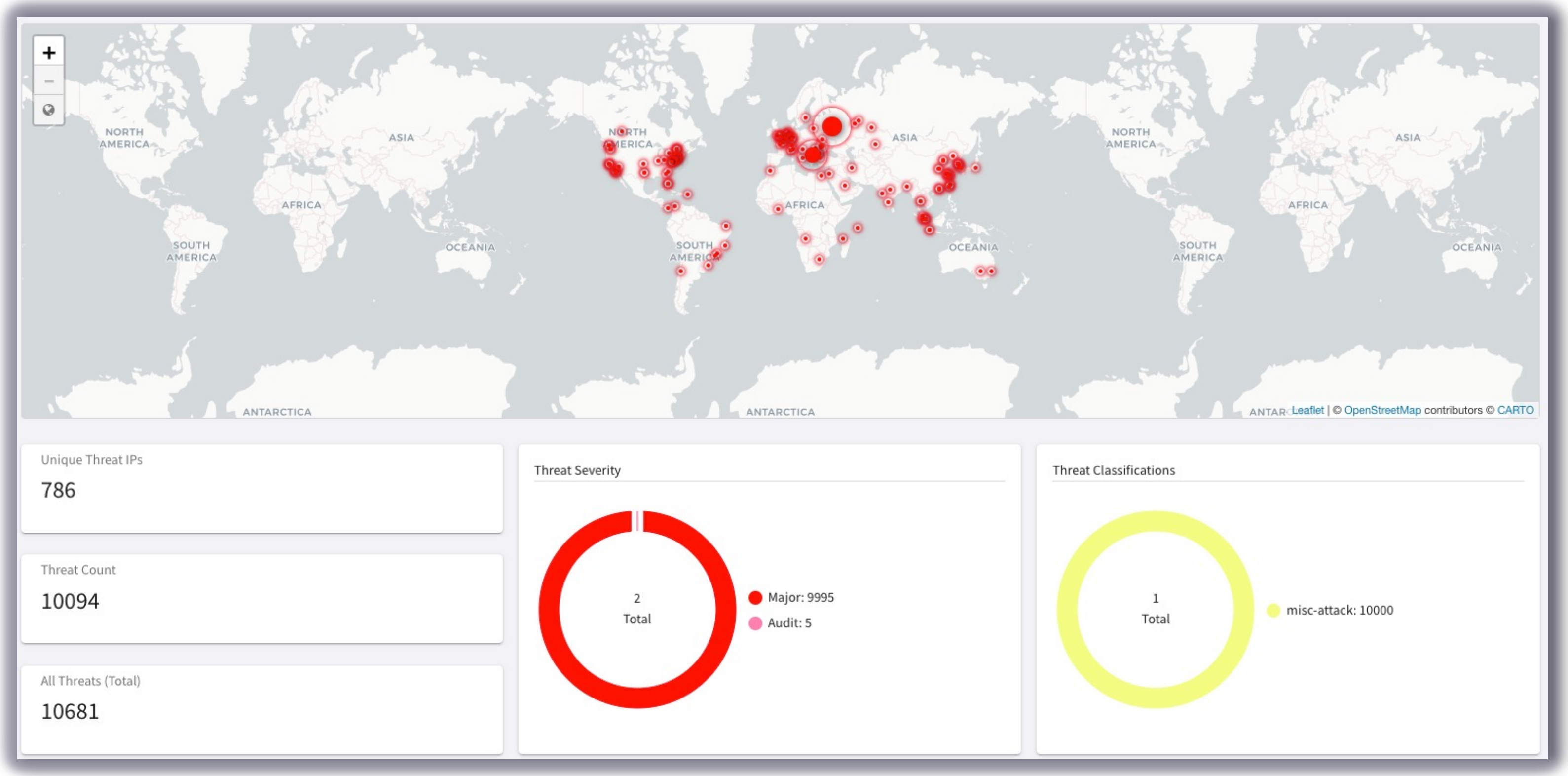
IDENTIFY AND REMEDIATE THREATS ACROSS MULTICLOUD NETWORKS

ACE Solutions Architecture Team

What is it?

aviatrix ACE Aviatrix Certified Engineer

- Multicloud native network security to dynamically **identify, alert, and remediate potential threats** to known malicious IP addresses
- **Distributed threat visibility** and control built into the network data-plane at every hop
- Identify potential **data exfiltration and compromised host**
- **No data-plane performance impact**
- **Complementary security solution** with full multicloud support



Unique Threat IPs
786

Threat Count
10094

All Threats (Total)
10681

Threat Severity

2 Total

● Major: 9995
● Audit: 5

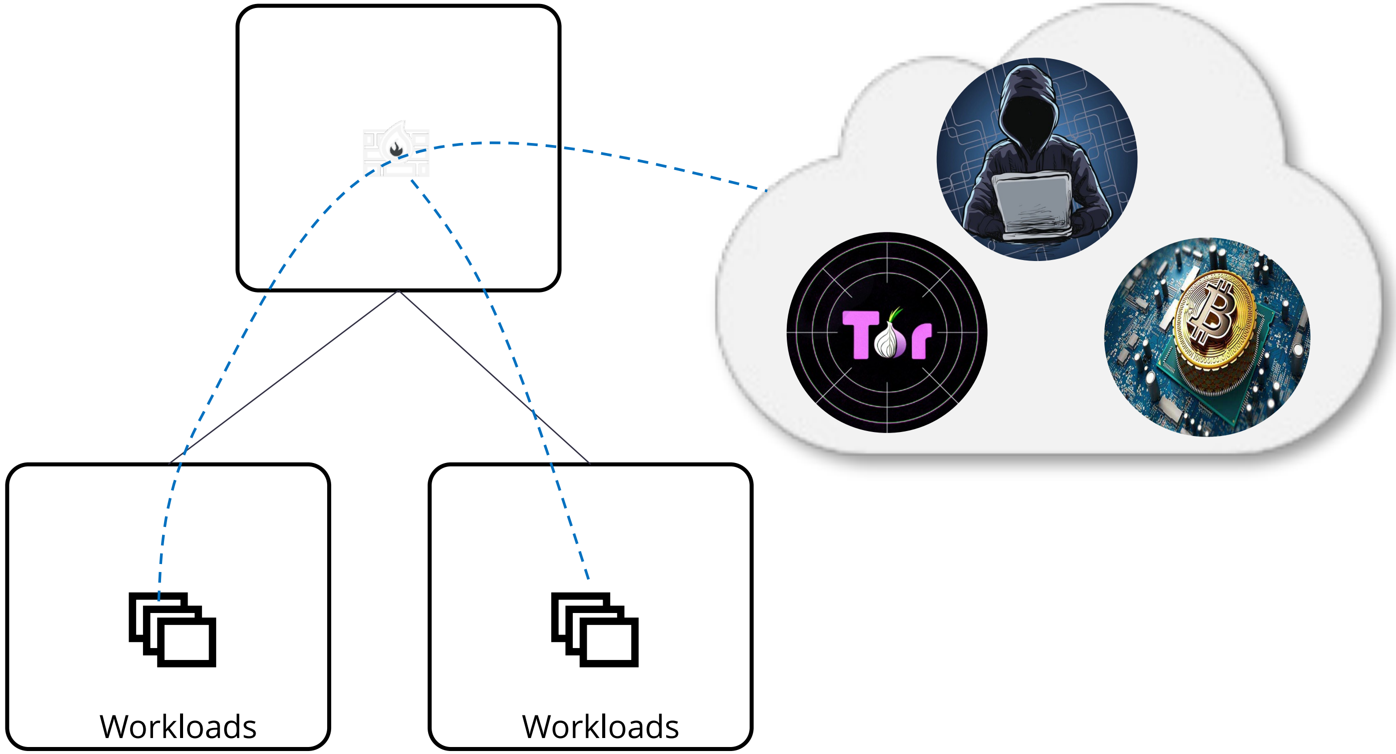
Threat Classifications

1 Total

● misc-attack: 10000

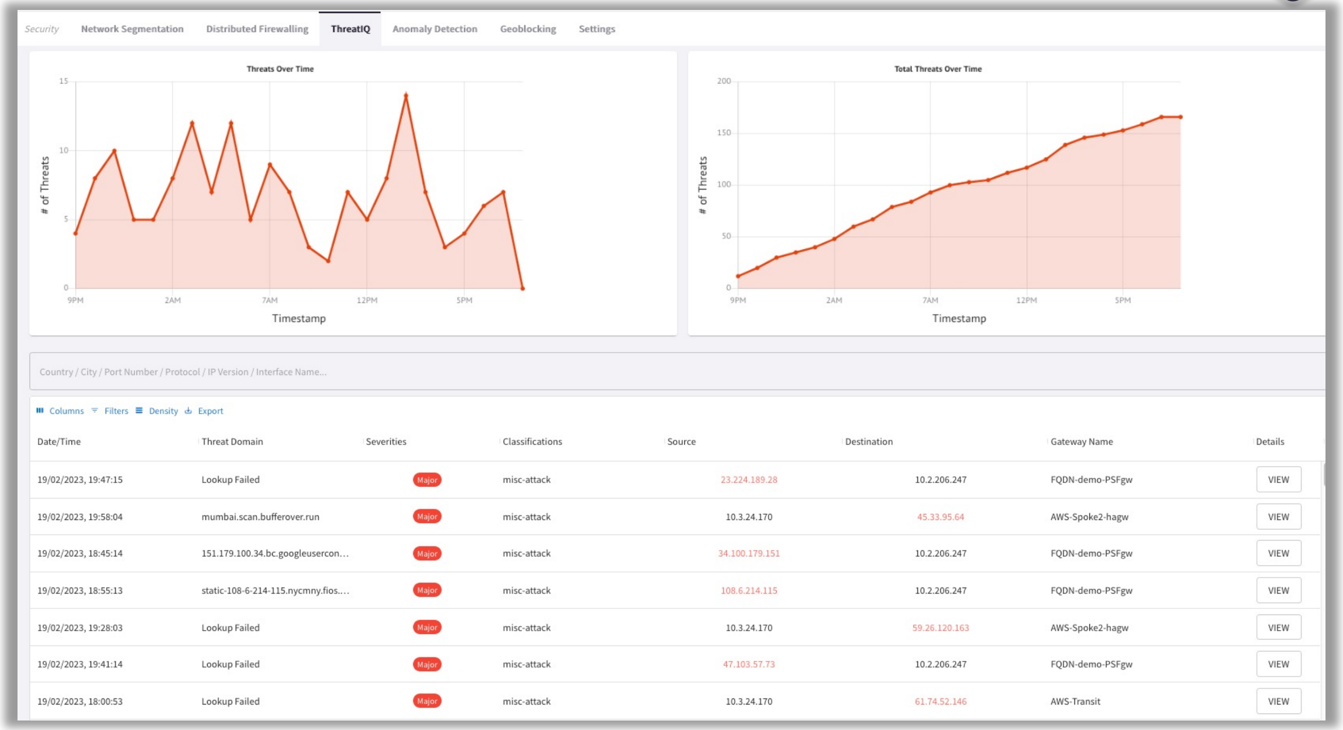
Why should enterprises care about it?

- Internet access is everywhere in the cloud and on by default for some CSPs
- Funneling traffic through choke points or 3rd party services is inefficient and ineffective
- Protect business from security risks associated with:
  - Data exfiltration
  - Botnets
  - Compromised hosts
  - Crypto mining
  - TOR
  - DDoS, and more

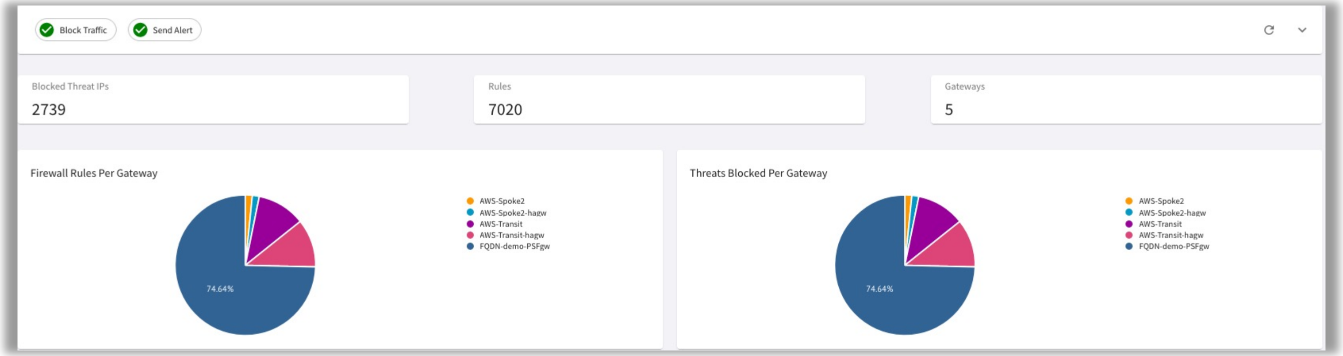


How does it work?

- **Distributed Inspection & Notification**
    - Aviatrix gateways across Multicloud environment send real-time NetFlow data to CoPilot
    - CoPilot analyzes the data on all public destinations against well-known Threat DB.
    - CoPilot alerts on any potential threats in the environment
    - CoPilot provides extreme visibility of the impacted communication flow
- **Distributed Enforcement**
    - CoPilot informs Aviatrix Controller to push firewall policies to all the Aviatrix gateways in the data path
    - Firewall policies automatically get updated with the current status of the threat.
    - Blocking threats with firewall policy is optional but recommended



Date/Time	Threat Domain	Severities	Classifications	Source	Destination	Gateway Name	Details
19/02/2023, 19:47:15	Lookup Failed	Major	misc-attack	23.224.189.28	10.2.206.247	FQDN-demo-PSFgw	VIEW
19/02/2023, 19:58:04	mumbai.scan.bufferover.run	Major	misc-attack	10.3.24.170	45.33.95.64	AWS-Spoke2-hagw	VIEW
19/02/2023, 18:45:14	151.179.100.34.bc.googleusercon…	Major	misc-attack	34.100.179.151	10.2.206.247	FQDN-demo-PSFgw	VIEW
19/02/2023, 18:55:13	static-108-6-214-115.nycmny.fios.…	Major	misc-attack	108.6.214.115	10.2.206.247	FQDN-demo-PSFgw	VIEW
19/02/2023, 19:28:03	Lookup Failed	Major	misc-attack	10.3.24.170	59.26.120.163	AWS-Spoke2-hagw	VIEW
19/02/2023, 19:41:14	Lookup Failed	Major	misc-attack	47.103.57.73	10.2.206.247	FQDN-demo-PSFgw	VIEW
19/02/2023, 18:00:53	Lookup Failed	Major	misc-attack	10.3.24.170	61.74.52.146	AWS-Transit	VIEW

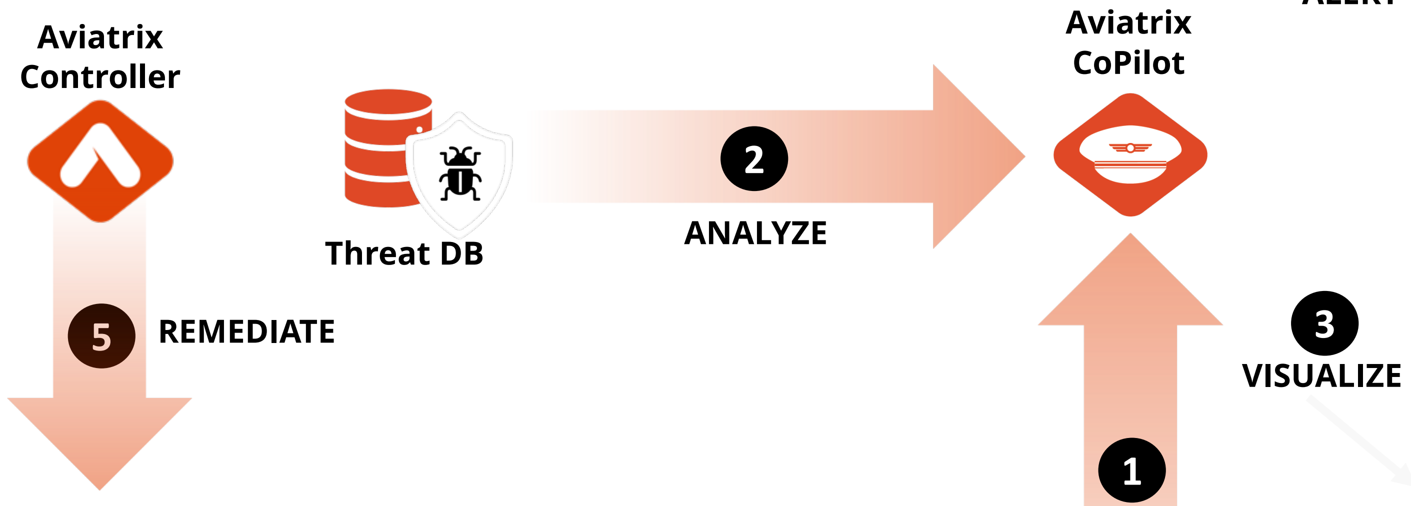


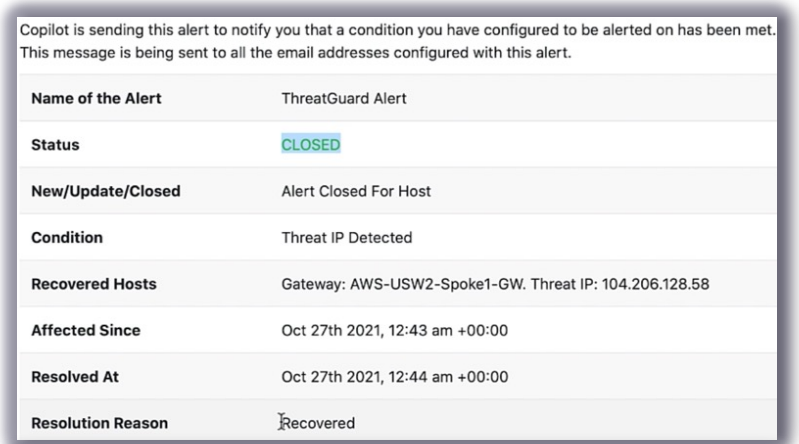
Blocked Threat IPs: 2739

Rules: 7020

Gateways: 5

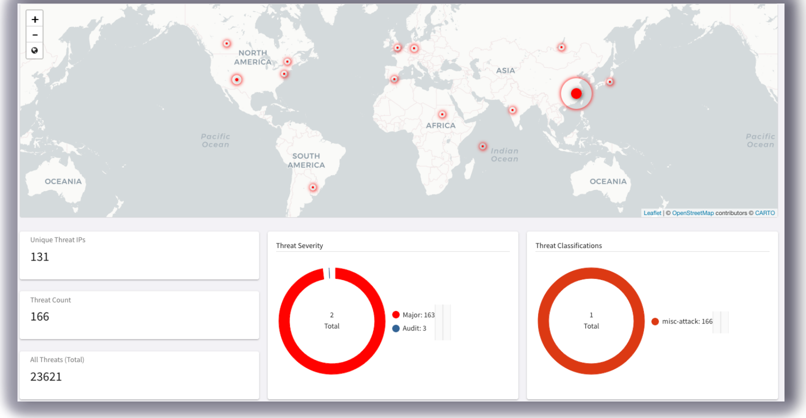
Workflow





Copilot is sending this alert to notify you that a condition you have configured to be alerted on has been met. This message is being sent to all the email addresses configured with this alert.

Name of the Alert	ThreatGuard Alert
Status	CLOSED
New/Update/Closed	Alert Closed For Host
Condition	Threat IP Detected
Recovered Hosts	Gateway: AWS-USW2-Spoke1-GW. Threat IP: 104.206.128.58
Affected Since	Oct 27th 2021, 12:43 am +00:00
Resolved At	Oct 27th 2021, 12:44 am +00:00
Resolution Reason	Recovered



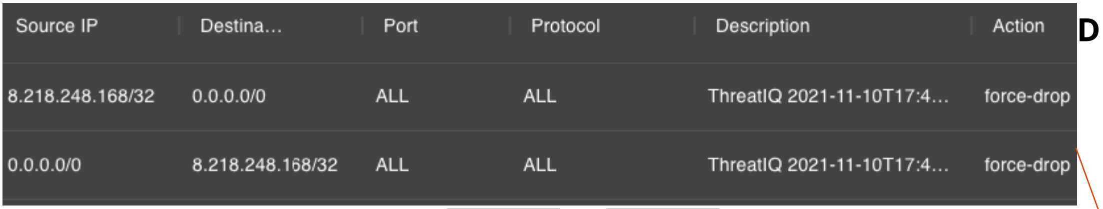
Unique Threat IPs
131

Threat Count
166

All Threats (Total)
23621

Threat Severity
- ● Major: 163
- ● Audit: 3

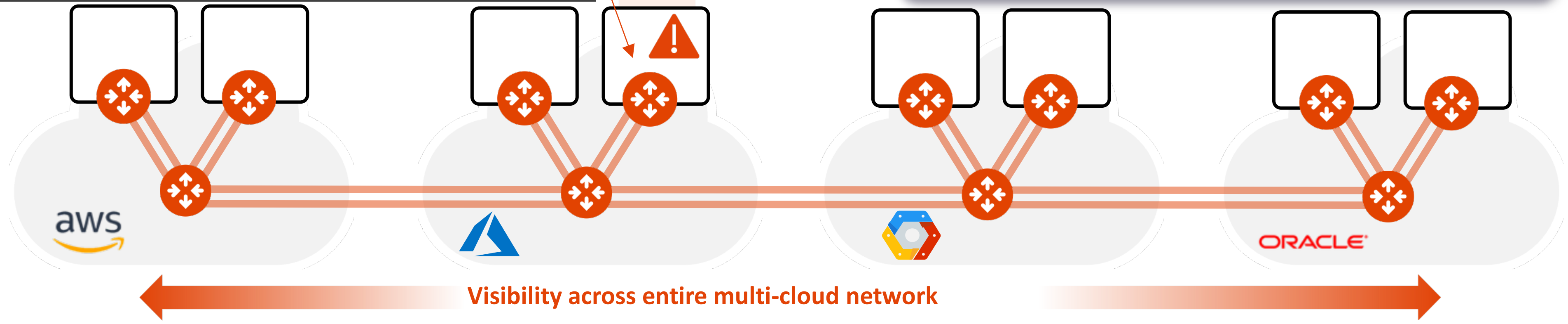
Threat Classifications
- ● misc-attack: 166



Source IP	Destina...	Port	Protocol	Description	Action
8.218.248.168/32	0.0.0.0/0	ALL	ALL	ThreatIQ 2021-11-10T17:4...	force-drop
0.0.0.0/0	8.218.248.168/32	ALL	ALL	ThreatIQ 2021-11-10T17:4...	force-drop

Firewall Rules

1
DISCOVER



Visibility across entire multi-cloud network

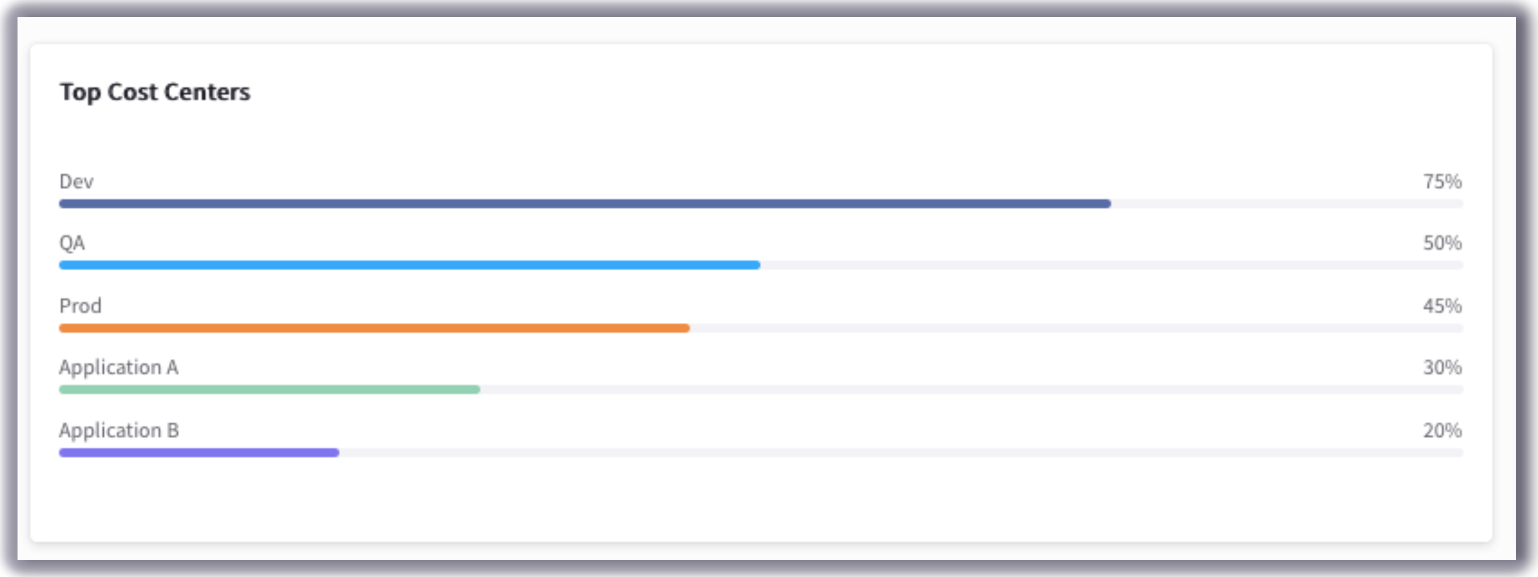
CostIQ

MONITORING THE COST OF YOUR BUSINESS UNITS

ACE Solutions Architecture Team

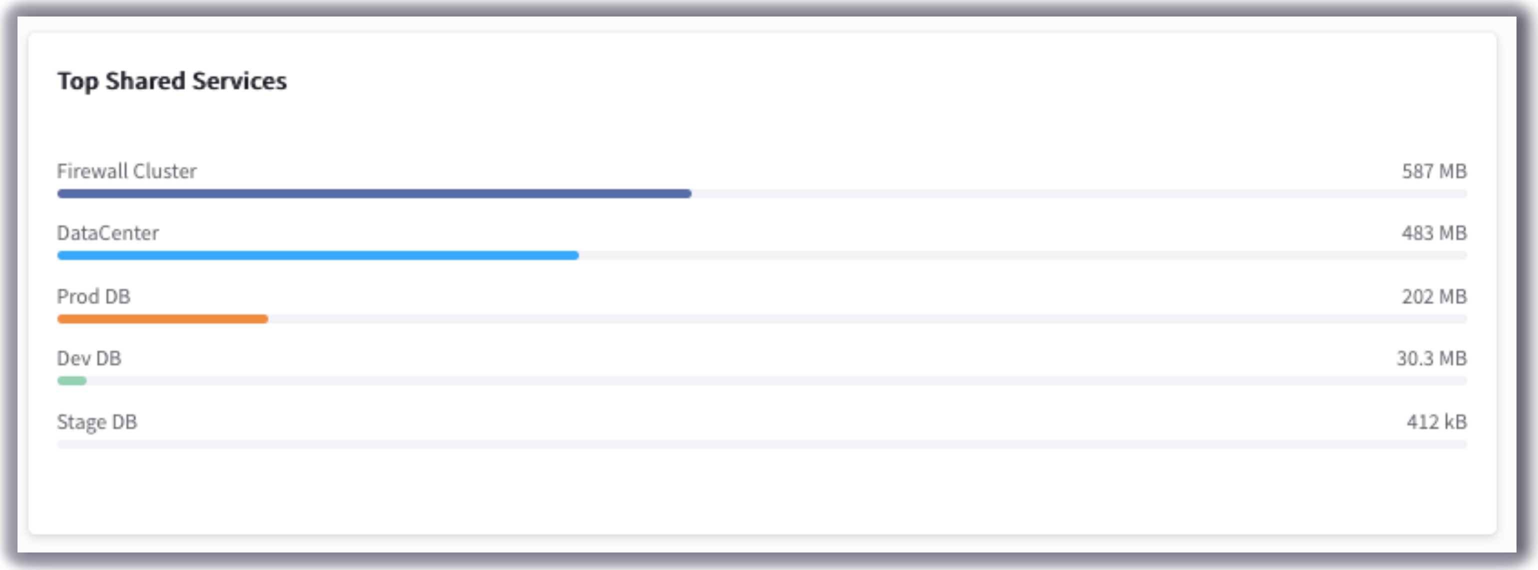
What is it?

- The **CostIQ** feature provides detailed traffic distribution analysis for your cost centers, including traffic flowing to shared-service resource hosts by Cloud Account, by Cost Center, by VPC/VNet, and by Gateway.
- The cost information displayed in CostIQ is grouped by:
  - **Cost Center** - A group of resources categorized by CSP (Cloud Service Provider) tags, associated VPCs/VNets. These CoPilot Cost Centers contain resources used by your real-life cost centers or business units.
  - **Shared Service** - A cloud or network resource shared by multiple teams or cost centers. You define Shared Services by listing the IP addresses or IP CIDR ranges of the shared resource hosts.



Top Cost Centers

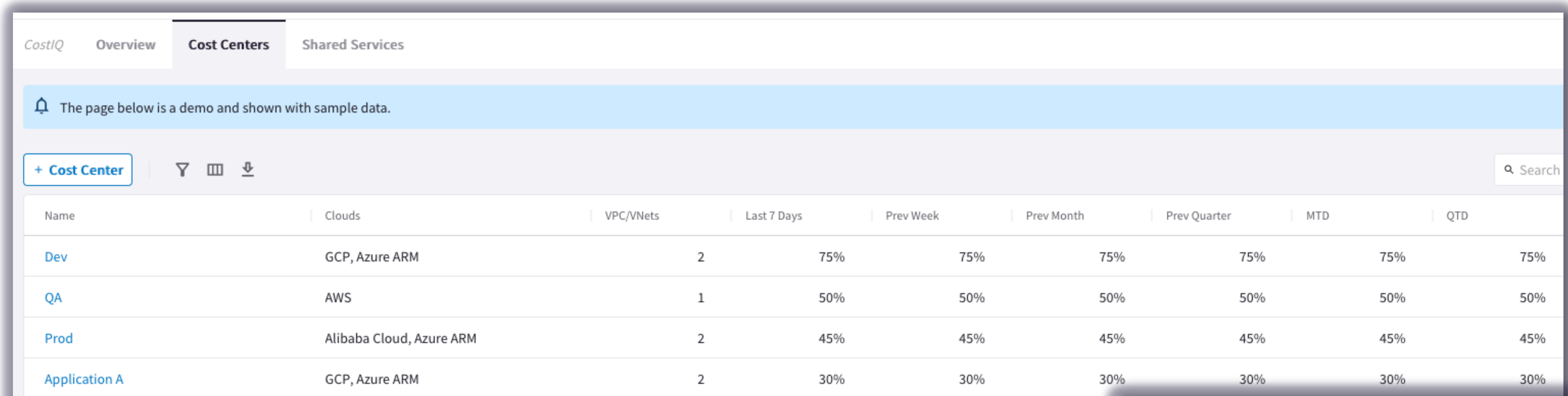
Dev	75%
QA	50%
Prod	45%
Application A	30%
Application B	20%



Top Shared Services

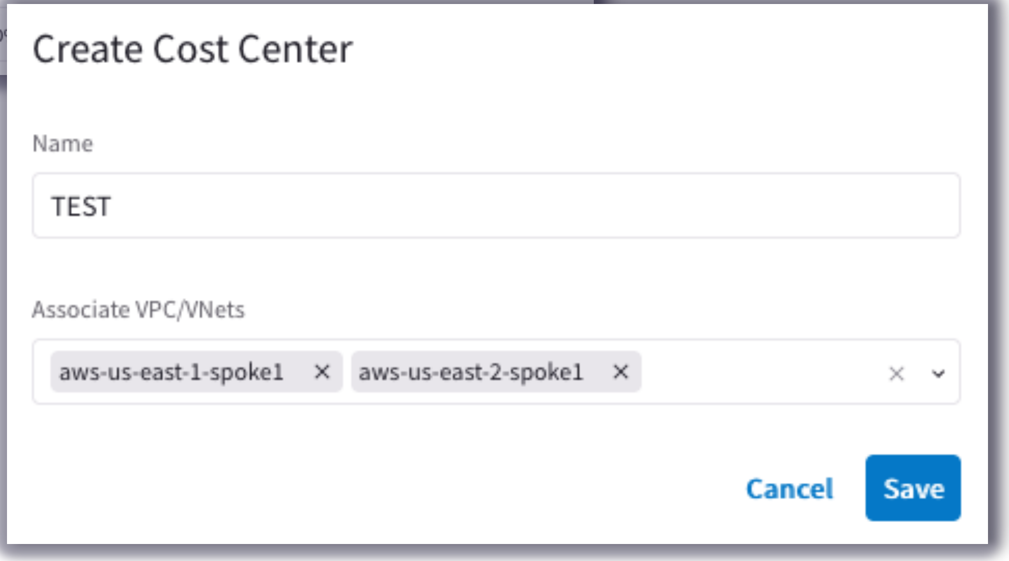
Firewall Cluster	587 MB
DataCenter	483 MB
Prod DB	202 MB
Dev DB	30.3 MB
Stage DB	412 kB

Cost Center (part.1)



The page below is a demo and shown with sample data.

Name	Clouds	VPC/VNets	Last 7 Days	Prev Week	Prev Month	Prev Quarter	MTD	QTD
Dev	GCP, Azure ARM	2	75%	75%	75%	75%	75%	75%
QA	AWS	1	50%	50%	50%	50%	50%	50%
Prod	Alibaba Cloud, Azure ARM	2	45%	45%	45%	45%	45%	45%
Application A	GCP, Azure ARM	2	30%	30%	30%	30%	30%	30%
Application B	GCP, Azure ARM, Alibaba Cloud	3	20%	20%	20			



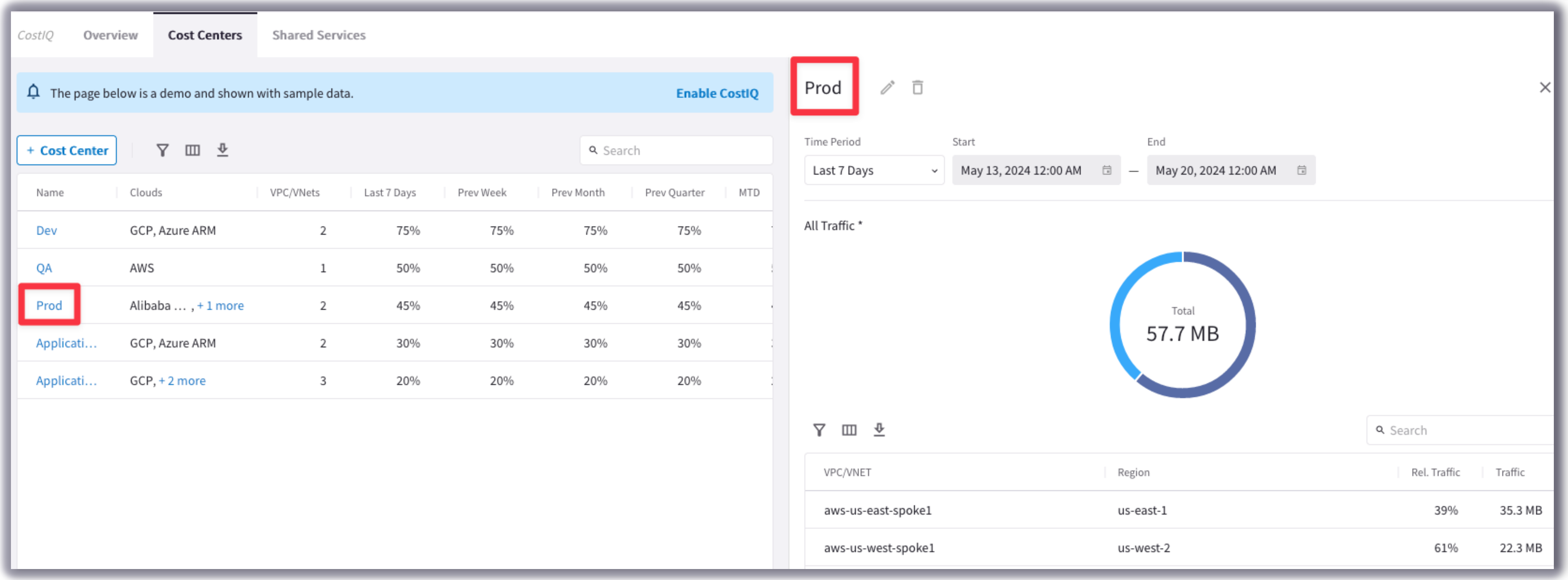
Create Cost Center

Name: TEST

Associate VPC/VNets: aws-us-east-1-spoke1 × aws-us-east-2-spoke1 ×

- The **Cost Center** is a logical grouping that represents a Line of Business or a department. Essentially, the Cost Center can embrace multiple VPCs/VNets across multiple clouds and multiple accounts.

Cost Center (part.2)



CostIQ Overview **Cost Centers** Shared Services

The page below is a demo and shown with sample data. **Enable CostIQ**

+ Cost Center

Search

Name	Clouds	VPC/VNets	Last 7 Days	Prev Week	Prev Month	Prev Quarter	MTD
Dev	GCP, Azure ARM	2	75%	75%	75%	75%	
QA	AWS	1	50%	50%	50%	50%	
Prod	Alibaba … , + 1 more	2	45%	45%	45%	45%	
Applicati…	GCP, Azure ARM	2	30%	30%	30%	30%	
Applicati…	GCP, + 2 more	3	20%	20%	20%	20%	

Prod

Time Period: Last 7 Days

Start: May 13, 2024 12:00 AM

End: May 20, 2024 12:00 AM

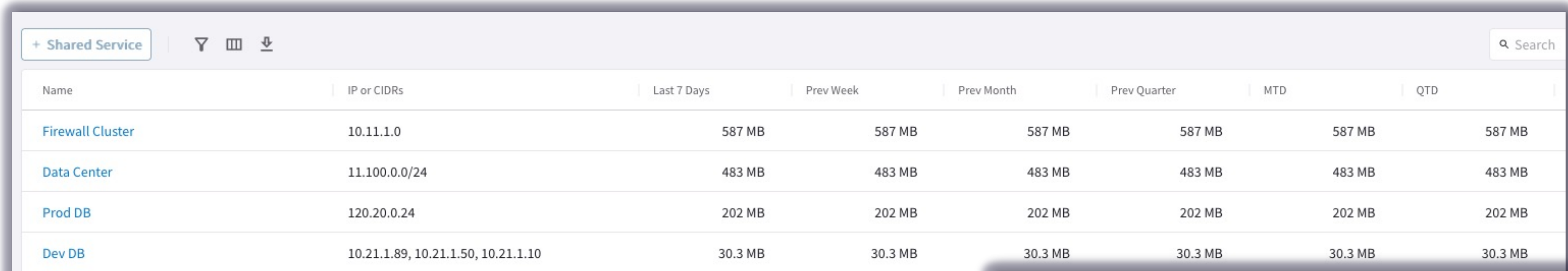
All Traffic *

Search

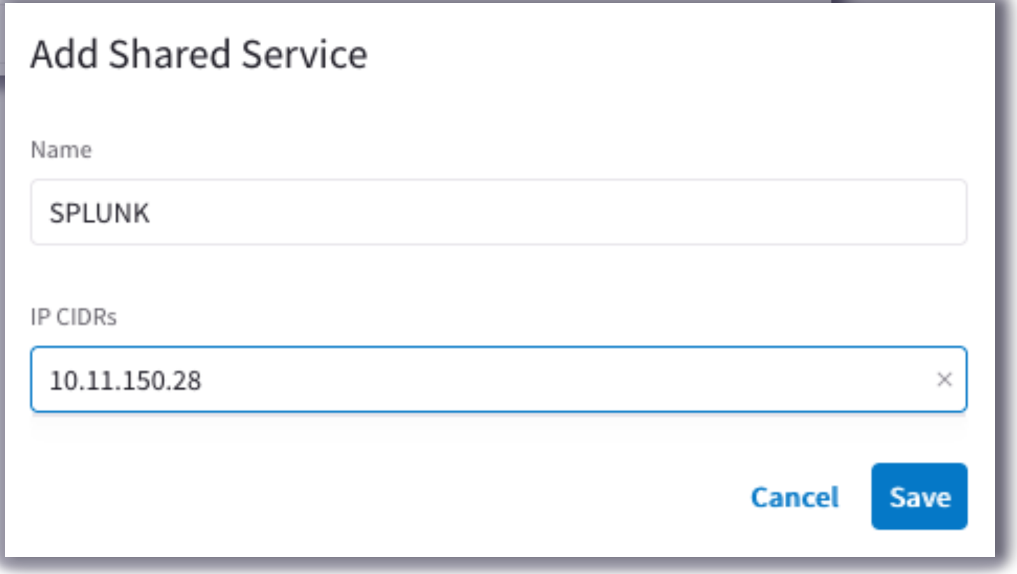
VPC/VNET	Region	Rel. Traffic	Traffic
aws-us-east-spoke1	us-east-1	39%	35.3 MB
aws-us-west-spoke1	us-west-2	61%	22.3 MB

- After defined a Cost Center, you can investigate all the associated Application VPCs/VNets that are all part of that Cost Center. You can drill down and find out the **relative amount of traffic** for each Application VPC/Vnet.

Shared Center (part.1)



Name	IP or CIDRs	Last 7 Days	Prev Week	Prev Month	Prev Quarter	MTD	QTD
Firewall Cluster	10.11.1.0	587 MB	587 MB	587 MB	587 MB	587 MB	587 MB
Data Center	11.100.0.0/24	483 MB	483 MB	483 MB	483 MB	483 MB	483 MB
Prod DB	120.20.0.24	202 MB	202 MB	202 MB	202 MB	202 MB	202 MB
Dev DB	10.21.1.89, 10.21.1.50, 10.21.1.10	30.3 MB	30.3 MB	30.3 MB	30.3 MB	30.3 MB	30.3 MB
Stage DB	10.21.1.90	412 kB	412 kB				



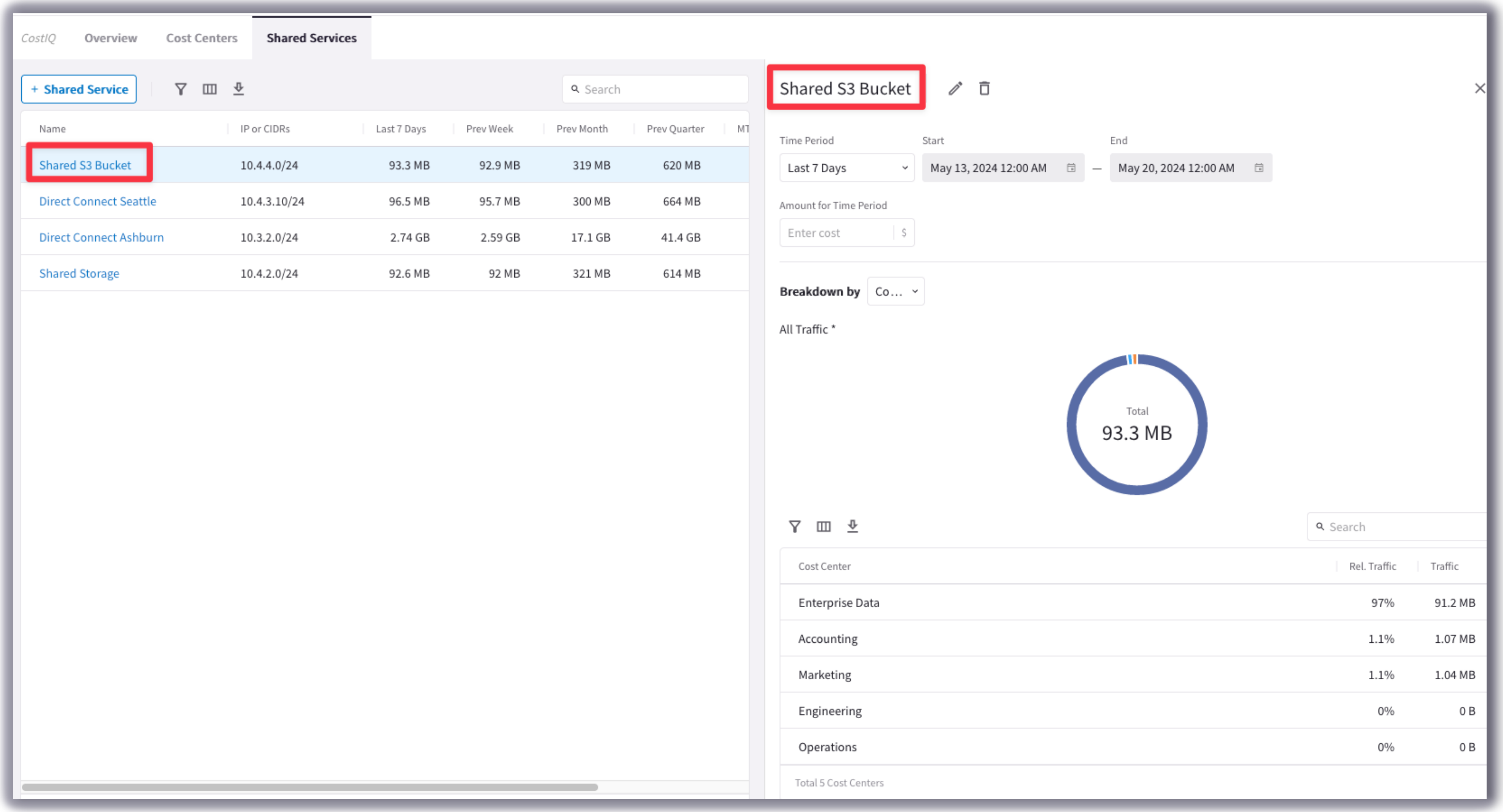
Add Shared Service

Name: SPLUNK

IP CIDRs: 10.11.150.28

- The **Shared Service** is another logical grouping that represents a Shared Application, for instance a syslog collector like Splunk. You can also associate S3 buckets to your Shared Services.
- The Shared Service allows you to monitor the resources that try reaching your shared applications

Shared Center (part.2)



Name	IP or CIDRs	Last 7 Days	Prev Week	Prev Month	Prev Quarter	MT
Shared S3 Bucket	10.4.4.0/24	93.3 MB	92.9 MB	319 MB	620 MB	
Direct Connect Seattle	10.4.3.10/24	96.5 MB	95.7 MB	300 MB	664 MB	
Direct Connect Ashburn	10.3.2.0/24	2.74 GB	2.59 GB	17.1 GB	41.4 GB	
Shared Storage	10.4.2.0/24	92.6 MB	92 MB	321 MB	614 MB	

Shared S3 Bucket

Time Period: Last 7 Days

Start: May 13, 2024 12:00 AM — End: May 20, 2024 12:00 AM

Amount for Time Period: Enter cost $

Breakdown by: Co…

All Traffic *

Total 93.3 MB

Cost Center	Rel. Traffic	Traffic
Enterprise Data	97%	91.2 MB
Accounting	1.1%	1.07 MB
Marketing	1.1%	1.04 MB
Engineering	0%	0 B
Operations	0%	0 B

Total 5 Cost Centers

- After defining a **Shared Service**, you can accurately find out what LOB/Department has been utilizing it.

aviatrix

ACE

Aviatrix Certified Engineer

Next: Lab 9 – ThreatIQ and CostIQ